FortiOS™ Handbook - FortiView

VERSION 5.2.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July-14-15

FortiOS™ Handbook - FortiView

01-523-122872-20150701

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-07-01	Official release.

Introduction

This document provides a general guide to FortiView, the FortiOS log view tool, explaining its layout, features, and its usefulness in everyday administrative scenarios.

The following chapters are included in this document:

Overview on page 7 outlines the role FortiView plays in FortiOS and its overall layout. This section also identifies which FortiGate platforms support the full FortiView features.

Sources on page 14 explains the features of FortiView's Sources console, and shows how you can investigate an unusual spike in traffic to determine which user is responsible.

Applications on page 15 explains the features of FortiView's Applications console and shows how you can view what sort of applications their employees are using.

Cloud Applications on page 15 explains the features of FortiView's Cloud Applications console and shows how you can drill down to access detailed data on cloud application usage, e.g. YouTube.

Destinations on page 16 explains the features of FortiView's Destinations console and shows how you can access detailed information on user destination-accessing through the use of drill down functionality.

Web Sites on page 17 explains the features of FortiView's Web Sites console and shows how you can investigate instances of proxy avoidance which is the use of a proxy site in order to access data that might otherwise be blocked by the server.

Threats on page 18 explains the features of FortiView's Threats console and shows how you can monitor threats to the network, both in terms of their Threat Score and Threat Level.

All Sessions on page 18 explains the features of FortiView's All Sessions console and shows how you can filter sessions by port number and application type.

Reference on page 22 explains reference information for the various consoles in FortiView, and describes the assortment of filtering options, drilldown options, and columns available.

Troubleshooting FortiView on page 33 offers solutions to common technical issues experienced by FortiGate users.

Overview

This section provides an overview of FortiView, its interface, and options, including the following:

Enabling FortiView

By default, FortiView is enabled on FortiGates running FortiOS firmware version 5.2 and above. You will find the FortiView consoles under **System > FortiView**. However, certain options will not appear unless the FortiGate has **Disk Logging** enabled.

Only certain FortiGate models support Disk Logging. A complete list of FortiGate platforms that support Disk Logging is provided in the matrix below.

To enable Disk Logging

1. Go to **Log & Report > Log Config > Log Settings** and select the checkbox next to **Disk**.
2. **Apply** the change.

To enable Disk Logging - CLI

```
config log disk setting
   set status enable
end
```

FortiView Feature Support - Platform Matrix

Note that the following table identifies three separate aspects of FortiView in FortiOS 5.2.3:

- Basic feature support
- Historical Data
- Disk Logging

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-20C Series	✔		
FG/FWF-30D/40C Series	✔		
FG/FWF-60C Series	✔		

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG/FWF-60D Series	✔		
FGR-60D	✔		
FG-60D	✔		
FG/FWF-80C Series	✔		
FG-80D	✔	✔	1 hour
FG/FWF-90D Series	✔	✔	1 hour
FG/FWF-92D Series	✔		
FG-110C	✔		
FG-111C	✔	**CLI**	1 hour
FG-100D Series	✔	✔	24 hours
FG-200B Series	✔	**#**	**#** (24 hours)
FG-200D Series	✔	✔	24 hours
FG-310B	✔		**#** (24 hours)
FG-311B	✔		**#** (24 hours)
FG-300C	✔	✔	24 hours
FG-300D	✔	✔	24 hours
FG-500D	✔	✔	24 hours
FG-620B	✔	**#**	**#** (24 hours)
FG-621B	✔	**#**	**#** (24 hours)
FG-600C	✔	✔	24 hours
FG-800C	✔	✔	24 hours
FG-1000C	✔	✔	24 hours
FG-1500D	✔	✔	24 hours
FG-1240B	✔	✔	24 hours

Platform	Basic Feature Support	Disk Logging	Historical Data *
FG-3016B	✔	**#**	**#** (24 hours)
FG-3040B	✔	**CLI**	24 hours
FG-3140B	✔	**CLI**	24 hours
FG-3240C	✔	**CLI**	24 hours
FG-3600C	✔	**CLI**	24 hours
FG-3700D	✔	**CLI**	24 hours
FG-3810A	✔	**#**	**#** (24 hours)
FG-3950B	✔	**#, CLI**	**#** (24 hours)
FG-3951B	✔	**#, CLI**	**#** (24 hours)
FG-5001A	✔	**#, CLI**	**#** (24 hours)
FG-5001B	✔	**CLI**	24 hours
FG-5001C	✔	**CLI**	24 hours
FG-5001D	✔	**CLI**	24 hours
FG-5101C	✔	**CLI**	24 hours
FS-5203B	✔	**CLI**	

✔ = *Default support.*
= *Local storage required.*

* Refer to section on Historical Data below.

Basic feature support

FortiView's consoles give insight into your user's traffic, not merely showing which users are creating the most traffic, but what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network.

FortiView basic feature support consists of the following consoles:

- Sources
- Applications
- Destinations
- All Sessions

The complete array of features in FortiView requires disk logging enabled (see below). It includes those consoles listed above as well as the following:

- Cloud Applications
- Web Sites
- Threats
- System Events
- Admin Logins
- VPN

Historical Data

Not all FortiView consoles have the same available historical data options, depending on whether or not your traffic is locally stored.

Below is a table showing which features are available for units using local storage, including the historical data options.

Only FortiGate models 100D and above support the 24 hour historical data.

Features	With Local Storage				Without Local Storage			
	Now	5 min	1 hr	24 hr *	Now	5 min	1 hr	24 hr
Sources	✔	✔	✔	✔	✔			
Applications	✔	✔	✔	✔	✔			
Cloud Applications	✔	✔	✔	✔	✔			
Destinations	✔	✔	✔	✔	✔			
Websites	✔	✔	✔	✔				
Threats		✔	✔	✔				
All Sessions	✔	✔	✔	✔	✔			
System Events		✔	✔	✔				
Admin Logins		✔	✔	✔				
VPN		✔	✔	✔				

* Not available for desktop models with SSD.

Disk Logging

Only certain FortiGate models support Disk Logging (see above).

To enable Disk Logging, go to **Log & Report > Log Config > Log Settings**, and select the checkbox next to **Disk** and apply the change.

Configuration Dependencies

Most FortiView consoles require the user to enable several features to produce data. The following table summarizes the dependencies:

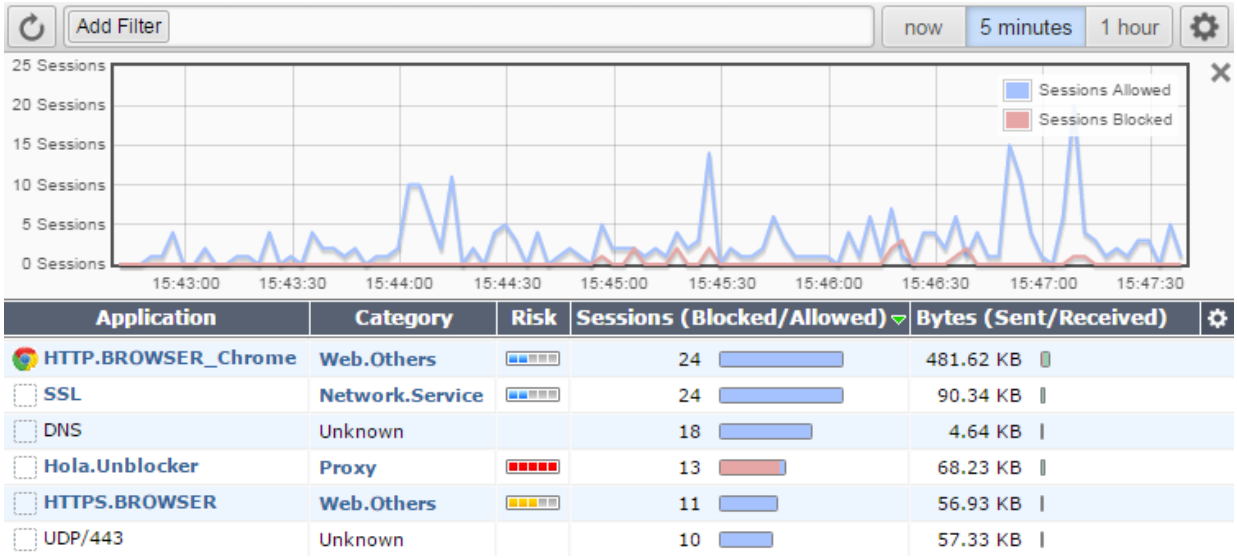
Feature	Dependencies (Realtime)	Dependencies (Historical)
Sources	None, always supported	Disk logging enabled Traffic logging enabled in policy
Applications	None, always supported	Disk logging enabled Traffic logging enabled in policy Application control enabled in policy
Cloud Applications	Not supported	Disk logging enabled Application control enabled in policy SSL "deep inspection" enabled in policy Deep application inspection enabled in application sensor Extended UTM log enabled in application sensor
Destinations	None, always supported	Disk logging enabled Traffic logging enabled in policy
Web Sites	Disk logging enabled Web Filter enabled in policy "web-url-log" option enabled in Web Filter profile	Disk logging enabled Web Filter enabled in policy "web-url-log" option enabled in Web Filter profile
Threats	Not supported	Disk logging enabled Traffic logging enabled in policy Threat weight detection enabled
All Sessions	None, always supported	Disk logging enabled Traffic logging enabled in policy

Feature	Dependencies (Realtime)	Dependencies (Historical)
System Events	Not supported	
Admin Logins	Not supported	
VPN	Not supported	
FortiSandbox	Not supported	

FortiView interface

FortiView lets you access information about the traffic activity on your FortiGate, visually and textually. FortiView is broken up into several consoles, each of which features a top menu bar and a graph window, as seen in the following image:

FortiView Application console sorted by Sessions (Blocked/Allowed)



The top menu bar features a **Refresh** button, which updates the data displayed, a **Filter** button for filtering the data by category, **Time Display** options (now, 5 minutes, 1 hour, or 24 hours), and a **Settings** button (containing additional viewing settings and a link to the Threat Weight menu).

The graph window can be hidden using the **X** in the top right corner, and re-added by selecting **Show Graph**. To zoom in on a particular section of the graph, **click and drag** from one end of the desired section to the other. This will appear in the **Time Display** options as a **Custom** selection. The minimum selection size is 60 seconds.

Only FortiGate models 100D and above support the 24 hour historical data.

FortiView consoles

This section describes the following log filter consoles available in FortiView:

Sources

The **Sources** console provides information about the sources of traffic on your FortiGate unit. This console can be filtered by Destination Interface, Policy, Security Action, Source Device, Source Interface, and Source IP.

Specific devices and time periods can be selected and drilled down for deep inspection.

Scenario: Investigating a spike in traffic

A system administrator notices a spike in traffic and wants to investigate it. From the **Sources** window, they can determine which user is responsible for the spike by following these steps:

1. Go to **System > FortiView > Sources**.
2. In the graph display, click and drag across the peak that represents the spike in traffic.
3. Sort the sources by bandwidth use by selecting the **Bytes (Sent/Received)** header.
4. Drill down into whichever source is associated with the highest amount of bandwidth use by double-clicking it. From this screen, you have an overview of that source's traffic activity.
5. Again, in either the **Applications** or **Destinations** view, select the **Bytes (Sent/Received)** header to sort by bandwidth use.
6. Double-click the top entry to drill down to the final inspection level, from which you can access further details on the application or destination, and/or apply a filter to prohibit or limit access.

Only FortiGate models 100D and above support the 24 hour historical data.

Applications

The **Applications** console provides information about the applications being used on your network. This console can be filtered by Application, Destination Interface, Policy, Security Action, and Source Interface.

Specific devices and time periods can be selected and drilled down for deep inspection.

In order for information to appear in the **Applications** console, Application Control must be enabled in a policy.

Scenario: Viewing application usage

A manager is interested in the office internet habits of their employees:

1. Go to **System > FortiView > Applications**, to view the list of applications accessed by the users on your network. Use the time-frame options to view what applications were used in those time periods (from now, 5 minutes, 1 hour, or 24 hours).
2. From **Sessions (Blocked/Allowed)** and **Bytes (Sent/Received)**, you can see how much traffic has been generated. Click these columns to show the traffic in descending order.
3. You notice that a social media application has created the most traffic of all the applications, and so it's at the top of the list. Drill down into the application by double-clicking, or right-click and select **Drill down to details...**.
4. You are directed to a summary page of the social media application. From here, you can see which specific user has made the most use of the application.

Only FortiGate models 100D and above support the 24 hour historical data.

Cloud Applications

The **Cloud Applications** console provides information about the cloud applications being used on your network. This includes information such as:

- The names of videos viewed on YouTube (visible by hovering the cursor over the session entry)
- Filed uploaded and downloaded from cloud hosting services such as Dropbox
- Account names used for cloud services

Two different views are available for the Cloud Applications: **Applications** and **Users** (located in the top menu bar next to the time periods). **Applications** shows a list of the programs being used. **Users** shows information

on the individual users of the cloud applications, including the username, if the FortiGate was able to view the login event.

This console can be filtered by Cloud Application.

In order for information to appear in the **Cloud Applications** console, an application control profile (that has Deep Inspection of Cloud Applications turned on) must be enabled in a policy, and SSL Inspection must use `deep-inspection`.

Scenario: Viewing cloud application usage data

From the Cloud Applications console, users can drill down to access detailed data on cloud application usage data. In this scenario, the console is used to determine the network's most frequent user of YouTube over a 24-hour period, and find out more about their usage patterns.

1. Go to **System > FortiView > Destinations**.
2. Select **Applications** view from the top menu bar if it is not already selected.
3. Select **24 Hours** from the Time Display options.
4. Find **YouTube** under the Application column and double-click it (or right-click and select **Drill down for details...**). This will open the YouTube stats window.
5. To determine the user who has accessed YouTube the most frequently, sort the column entries by **Sessions** by selecting the column header of the same name.
6. Double-click (or right-click and select **Drill down for details...**) the top-bandwidth YouTube user to view detailed stats, including the names of videos watched by the user and the date and time each video was accessed.

Only FortiGate models 100D and above support the 24 hour historical data.

Destinations

The **Destinations** console provides information about the destination IP addresses of traffic on your FortiGate unit, as well as the application used. You can drill down the displayed information, and also select the device and time period, and apply search filters.

This console can be filtered by Destination Interface, Destination IP, Policy, Security Action, and Source Interface.

Scenario: Monitoring destination data

The Destinations console can be used to access detailed information on user destination-accessing through the use of the console's drilldown functionality. In this scenario, the console is used to find out more about a particular user's Facebook usage patterns over a 24-hour period:

1. Go to **System > FortiView > Destinations**.
2. Select **1 hour** from the Time Display options at the top right corner of the console.
3. The easiest way to locate most destinations is to scan the Applications column for the name of the application. Once the session containing Facebook has been located, double-click it to access the Destination summary window.
4. Locate Facebook in the Applications column and double-click it to view the Facebook drilldown page. From here, detailed information regarding the user's Facebook session can be accessed.

Only FortiGate models 100D and above support the 24 hour historical data.

Web Sites

The **Web Sites** console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand.

This dashboard can be filtered by Domain.

In order for information to appear in the **Web Sites** console, web filtering must be enabled in a policy, with FortiGate Categories enabled.

Scenario: Investigating an instance of Proxy Avoidance

In this scenario, the Categories view will be used to investigate an instance of Proxy Avoidance, one of the Categories recognized by FortiOS. Proxy Avoidance denotes the use of a proxy site in order to access data that might otherwise be blocked by the server.

1. Go to **System > FortiView > Web Sites** to open the Web Sites console.
2. Select **Categories** from the top bar menu to enter Categories view.
3. Scan the **Categories** column and locate the instance of Proxy Avoidance, then double-click it to enter its drill down screen.

Only FortiGate models 100D and above support the 24 hour historical data.

Threats

The **Threats** console lists the top users involved in incidents, as well as information on the top threats to your network.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus

The console can be filtered by Destination Interface, Policy, Security Action, Source Interface, Threat, and Threat Type.

In order for information to appear in the **Threats** console, Threat Weight Tracking must be enabled.

Scenario: Monitoring Threats to the Network

Some users have high Threat Scores. The Threats console can be used to view all threats and discover why such high scores are being shown:

1. In the graph display, click and drag across the peak that represents the spike in threat score.
2. Sort the threats by score or level by selecting the **Threat Score (Blocked/Allowed** or the **Threat Level** headers respectively.
3. You see that a specific threat's Threat Level is at Critical. Drill down into the threat by double-clicking, or right-click and select **Drill down to details...**.
4. From this summary page, you can view the source IPs and the number of sessions that came from this threat. Double-click on one of them.
5. The following page shows a variety of statistics, including **Reference**. The URL next to it will link you to a FortiGuard page where it will display the description, affected products, and recommended actions, if you are not familiar with the particular threat.

Only FortiGate models 100D and above support the 24 hour historical data.

All Sessions

The **All Sessions** console provides information about all FortiGate traffic. This console can be filtered by Application, Checksum, Destination Interface, Destination IP, Policy, Security Action, Source Device, Source

Interface, Source IP, Threat, and Threat Type.

This console has the greatest number of column options to choose from. To choose which columns you wish to view, select the column settings cog at the far right of the columns and select your desired columns. They can then be clicked and dragged in the order that you wish them to appear.

A number of columns available in FortiView are only available in All Sessions. For example, the **Action** column displays the type of response taken to a security event. This function can be used to review what sort of threats were detected, whether the connection was reset due to the detection of a possible threat, and so on. This would be useful to display alongside other columns such as the **Source**, **Destination**, and **Bytes (Sent/Received)** columns, as patterns or inconsistencies can be analyzed.

Similarly, there are a number of filters that are only available in All Sessions, one of which is **Protocol**. This allows you to display the protocol type associated with the selected session, e.g. TCP, FTP, HTTP, HTTPS, and so on.

Scenario: Filtering sessions by port number and application type

From the **All Sessions** console, a wide variety of filters can be applied to sort the session data. In this example, the All Sessions filters will be used to locate a specific user's recent Skype activity.

1. Go to **System > FortiView > All Sessions**.
2. Select **now** from the **Time Display** options if it is not already selected.
3. Select the **Filter** button, then select **Applications**. This will open a drop-down menu listing the applications that appear in the master session list. From this list, locate and select **Skype**, or type `Skype` into the search bar and hit **Enter**. This will filter the session list to only feature Skype usage.
4. Select the **Filter** button again, then select **Destination Port** from the drop-down menu, then locate and select the desired port number. This will add a second filter which will restrict the results to presenting only the Skype data associated with that port number.

Only FortiGate models 100D and above support the 24 hour historical data.

System Events

The **System Events** console lists security events detected by FortiOS, providing a name and description for the events, an assessment of the event's severity level (**Alert**, **Critical**, **Emergency**, **Error**, or **Warning**), and the number of instances the events were detected. This console can be filtered by Event Name and Severity.

Scenario: Viewing Security Events & Security Actions

System Events can be used in conjunction with All Sessions to see what network security events took place, and specifically see what action was taken upon their detection:

- Go to **System > FortiView > System Events**, to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.

- You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Note when the event took place, and go to **System > FortiView > All Sessions**, to see more information pertaining to the security event.
- From this console, you can determine the system event's source, how much traffic was sent and received, and the security action taken in response to this security event. These actions differ, depending upon the severity of the security event. To view these actions, see the table-entry for **Security Action** in Columns displayed on page 25.

Only FortiGate models 100D and above support the 24 hour historical data.

Admin Logins

The **Admin Logins** console provides information on administrator interactions with the network, including the number of login instances, number of failed logins, and the length of time logged in. This console can be filtered by User Name.

Scenario: Scrutinizing Administrator Security

Admin Logins can be used in conjunction with System Events to see who was on during a system change that impacted performance and allowed a threat to persist/pass through the firewall:

- Go to **System > FortiView > System Events**, to see what and how many network events have taken place, as well as how severe they are in terms of the threat they pose to the network.
- You see that a particular event has warranted a severe rating, and has allowed traffic to bypass the firewall. Double-click on the event to drill down.
- Once drilled down, you can see the date and time that the system change took place.
- Go to **System > FortiView > Admin Logins**, to see who has been logged in, how long they have been logged in, and what configuration changes they have made. Using the time graph, you can correlate the information from System Events with who was logged in at the time the threat was allowed.

Only FortiGate models 100D and above support the 24 hour historical data.

VPN

From the **VPN** console, users can access information on any VPNs associated with their FortiGate. From the initial window, a list of all the associated VPNs is provided, along with general information, such as number of user connections and VPN type. By double-clicking on an individual VPN (or right-clicking and selecting **Drill down for details...**), users can access more specific data on that VPN.

Logs in the VPN console can be sorted by number of connections, last connection time, or data sent/received by selecting the column headers.

This console can be filtered by User Name and VPN Type.

Certain dashboard options will not appear unless your FortiGate has Disk Logging enabled.

Furthermore, only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 7 for more information.

To enable Disk Logging, go to **Log & Report > Log Config > Log Settings**, and select the checkbox next to **Disk** and apply the change.

Scenario: Investigating VPN user activity

The VPN console can be used to access detailed data on VPN-user activity via the use of the drill down windows. In this scenario, the administrator looks into the usage patterns of the IPsec user who has most frequently connected to the network.

1. Go to **System > FortiView > VPN** to view the VPN console.
2. Select the **Connections** column header to sort the entries by number of connections to the network.
3. Locate the top user whose VPN Type is **ipsec** and double-click the entry to enter that user's drill down screen.
4. To get the most representative data possible, sort the entries by bandwidth use by selecting the **Bytes (Sent/Received)** column header. Double-click the top entry to enter the drill down window for that connection instance.
   From this screen, the administrator can find out more about the specific session, including the date/time of access, the XAuth (Extensible Authentication) User ID, the session's Tunnel ID, and more.

Reference

This section consists of reference information for the various consoles in FortiView. Each console has an assortment of filtering options, drilldown options, and columns that can be displayed. Since many of these options and columns persist through each console, the entire list of options and their descriptions is included below. Attempts have been made to identify the instances where an option or column is only available to a particular console.

This section includes:

Filtering options

When you select the **Add Filter** button, a drop-down list appears with a list of available filtering options. Available options differ based on which console is currently being viewed. The following table explains all of the available filtering options:

Filter option	Description
Application	Filter by application name.
Checksum	Filter by checksum value. Checksums are reference digits used to represent the correct datasum of a packet in order to detect errors.
Cloud Application	Filter by cloud application name. **Note:** This filter is only available in the **Cloud Applications** console.
Destination Interface	Filter by the interface type used by the destination user, e.g. wan1.
Destination IP	Filter by the IP address used by the destination.
Destination Port	Filter by the port used by the destination. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Domain	Filter by domain name. **Note:** This filter is only available in the **Web Sites** console.

Filter option	Description
Event Name	Filter by security event name. **Note:** This filter is only available in the **System Events** console.
File Name	Filter by file name. **Note:** This filter is only available in the **FortiSandbox** console.
NAT Source IP	Filter by the NAT-translated source IP address. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
NAT Source Port	Filter by the NAT-translated source interface. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Policy	Filter by the policy identification number.
Protocol	Filter by the protocol used by the source, e.g. tcp or udp. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Security Action	Filter by the type of response taken to the security event. The types of possible actions are as follows: **Allowed:** No threat was detected and the connection was let through. **Blocked:** A threat was detected and the connection was not let through. **Reset:** A possible issue was detected and the connection was reset. **Traffic Shape:** Some data packets may have been delayed to improve system-wide performance.
Severity	Filter by the severity level (**Critical**, **High**, **Medium** or **Low**) associated with a security event.
Source Device	Filter by source device type, e.g. mobile.
Source Interface	Filer by the interface type used by the source user, e.g. wan1.
Source IP	Filter by the source IP address.

Filter option	Description
Source Port	Filter by the source interface. **Note:** This filter is only available in the **All Sessions** console,(viewing the **now** time display).
Status	Filter by the maliciousness of a file. The types of possible status' are **Malicious**, **High**, **Medium**, **Low**, **Clean**, **Unknown**, and **Pending**. **Note:** This filter is only available in the **FortiSandbox** console.
Threat	Filter by threats received.
Threat Type	Filter by threat classification, e.g. DoS.
User Name	Filter by user name.
VPN Type	Filter by Virtual Private Network (VPN) protocol type, e.g. PPTP. **Note:** This filter is only available in the **VPN** console.

Drilldown options

Double-click, or right-click, on any entry in a FortiView console and select **Drill down to details...**, to view the following tabs (options vary depending on the console selected):

Drilldown option	Description
Applications	Select to drill down by application to view application-related information, including the application name, sessions blocked and allowed, bytes sent and received, and the risk level. You can sort entries by selecting the column header.
Destinations	Select to drill down by destination to view destination-related information, including the IP address and geographic region, interface, threat score, number of sessions blocked and allowed, and bytes sent and received. You can sort entries by selecting the column header.
Threats	Select to drill down by threat to view threat-related information, including the threat name, category, threat level, threat score, and number of sessions blocked and allowed. You can sort entries by selecting the column header.
Domains	Select to drill down by domain to view domain-related information, including domain name, category, browsing time, threat weight, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.

Drilldown option	Description
Categories	Select to drill down by category to view category-related information, including category name, browsing time, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.
Sessions	Select to drill down by sessions to view session-related information, including date/time, source, destination IP address and geographic region, application name,security action, security event, and bytes sent/received. You can sort entries by selecting the column header.
Sources	Select to drill down by rows to view source-related information, including IP address, device type, interface type, threat score, number of sessions blocked/allowed, and bytes sent/received. You can sort entries by selecting the column header.

Columns displayed

The following columns appear in the initial window of the consoles. Some columns may only be visible by selecting them from the column drop-down menu. Options also vary depending on the console selected.

Column name	Description
Action	Displays the type of response taken to a security event. The types of possible actions are as follows: • **Allowed**: No threat was detected and the connection was let through. • **Blocked**: A threat was detected and the connection was not let through. • **Reset**: A possible issue was detected and the connection was reset. • **Traffic Shape**: Some data packets may have been delayed to improve system-wide performance. **Note:** This column is only available in the **All Sessions** console.
Application	Displays the application name and service. When **Time Display** is set to **now**, you can access further information about an application by selecting the column entry.
Application Category	Displays the type of application used in the selected session, e.g. video player, social media. **Note:** This column is only available in the **All Sessions** console.
Application ID	Displays the identification number associated with the application used in the selected session. **Note:**This column is only available in the **All Sessions** console.

Column name	Description
Application Risk **Risk**	Displays the application risk level. You can hover the mouse cursor over the entry in the column for additional information, and select the column header to sort entries by level of risk. Risk uses a 5-point risk rating. The rating system is as follows: • **Critical**: Applications that are used to conceal activity to evade detection. • **High**: Applications that can cause data leakage, are prone to vulnerabilities, or may download malware. • **Medium**: Applications that can be misused. • **Elevated**: Applications that are used for personal communications or can lower productivity. • **Low**: Business-related applications or other harmless applications.
Browsing Time	Displays the amount of time a user has spent browsing a web site (in seconds). **Note:** This column is only available in the **Web Sites** console, in **Categories** view..
Bytes (Sent/Received)	Displays the size of sent and received data packets, as measured in bytes. Select the column header to sort the entries by size. **Note:** This information is available on some consoles as two separate columns: **Sent** and **Received**.
Category	Displays the category descriptor appropriate to whatever console is being displayed. For example, threat categories are displayed in the Threats console.
Clean	Displays the number of "clean" (safe) files found in the selected FortiSandbox session. **Note:** This column is only available in the **FortiSandbox** console, in **Source** view.
Cloud User	Displays the users accessing cloud applications by IP address. **Note:** This column is only available in the **Cloud Applications** console, in **Users** view.

Column name	Description
Configuration Changes	Displays the number of configuration changes made by the user. You can hover the mouse cursor over an entry for additional information. **Note:** This column is only available in the **Admin Logins** console.
Connections	Displays the number of VPN connections made by the selected user.. **Note:** This column is only available in the **VPN** console.
Destination	Displays the destination name, IP address and geographic region.
Destination Country	Displays the country session data is being sent to. **Note:** This column is only available in the **All Sessions** console.
Destination Interface	Displays which interface session data is being sent through, e.g. wan1.
Destination Port	Displays the port number of the destination server being used to accept data. Note: This column is only available in the **All Sessions** console.
Device	Displays the device IP address or Fully Qualified Domain Name (FQDN).
Domain	Displays the domain associated with the selected web site, e.g. google.com. **Note:** This column is only available in the **Web Sites** console.
DST Nat IP **NAT Destination**	Displays the Network Address Translation (NAT) IP address associated with the destination server. **Note:** This column is only available in the **All Sessions** console.
DST Nat Port **NAT Destination Port**	Displays the Network Address Translation (NAT) port number associated with the destination server. **Note:** This column is only available in the **All Sessions** console.
Duration	Displays the amount of time (in seconds) a user has been logged in. **Note:** This column is only available in the **Admin Logins** console.
Event Name (Description)	Displays the name and description of the selected security event. **Note:** This column is only available in the **System Events** console.

Column name	Description
Events	Displays the number of security events that occurred within a selected session. **Note**: This column is only available in the **System Events** console.
Expires	Displays the amount of time a session has (in seconds) before it is set to expire. **Note:** This column is only available in the **All Sessions** console, in **now** Time Display view.
Failed Logins	Displays the number of failed login attempts made by an administrator over the specified time period. **Note:** This column is only available in the **Admin Logins** console.
Files (Up/Down)	Displays the number of files uploaded and downloaded. Hover the mouse cursor over the entry in the column for additional information. **Note:** This column is only available in the **Cloud Applications** console.
FortiASIC	Displays the type of FortiASIC hardware acceleration used in the specified session, if present. **Note:** This column is only available in the **All Sessions** console, in the **now** Time Display view.
Group	Displays the group ID associated with the selected session. **Note:** This column is only available in the **All Sessions** console.
Last Connection Time	Displays the most recent instance of connection to the selected Virtual Private Network (VPN). **Note:** This column is only available in the **VPN** console.
Level **Threat Level**	Displays the threat level. Select the column header to sort entries by threat level.
Log ID	Displays the identification number for the data log associated with this entry. **Note:** This column is only available in the **All Sessions** console.

Column name	Description
Login IDs	Displays the number of login IDs associated with the selected cloud application. **Note:** This column is only available in the **Cloud Applications** console, in **Applications** view.
Logins	Displays the number of successful logins made by an administrator over the specified time period. **Note:** This column is only available in the **Admin Logins** console.
Policy ID	Displays the identification number of the policy under which the selected connection was allowed.
Policy UUID	Displays the Universally Unique Identifier (UUID) of the selected policy, if present. **Note:** This column is only available in the **All Sessions** console.
Protocol	Displays the protocol type associated with the selected session, e.g. TCP. **Note:** This column is only available in the **All Sessions** console.
Security Action	Displays the action taken in response to the selected security event. The types of possible actions are as follows: • **Allowed**: No threat was detected and the connection was let through. • **Blocked**: A threat was detected and the connection was not let through. • **Reset**: A possible issue was detected and the connection was reset. • **Traffic Shape**: Some data packets may have been delayed to improve system-wide performance.
Security Events	Displays the type of security event detected in the selected session. **Note**: This column only appears in the **All Sessions** console.
Sequence Number	Displays the TCP sequence number associated with the selected session. **Note**: This column only appears in the **All Sessions** console.
Service	Displays the ID of the service application in use in the selected session. **Note:** This column only appears in the **All Sessions** console.

Column name	Description
Sessions	Displays the number of sessions associated with the selected destination. **Note:** This column only appears in the **Destinations** console, in the **now** Time Display view.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked and allowed by FortiOs. In some consoles, entries can be sorted by number of sessions by selecting the column header..
Severity	Displays the severity level (**Critical**, **High**, **Medium** or **Low**) associated with the selected security event. **Note:** This column is only available in the **System Events** console.
Source	Displays the source IP address and/or user ID, if applicable.
Source Interface	Displays which interface is being used by the destination server (eg. wan1).
Source Port	Displays the port number being used by the source server to send data.
Src NAT IP **NAT Source**	Displays the Network Address Translation (NAT) IP address associated with the source server.
Src NAT Port **NAT Source Port**	Displays the Network Address Translation (NAT) port number associated with the source server.
Status	Displays the status of **Note:** This column is only available in the **FortiSandbox** console, in **Files** view.
Submittted	Displays the number of files submitted to the FortiSandbox for assessment in the selected session. **Note:** This column is only available in the **FortiSandbox** console, in **Files** view.
Threat	Displays the threat type detected in the selected session.
Threat Score (Blocked/Allowed)	Displays the threat score value, a measurement of the total number of threats detected over the course of the session. You can select the column header to sort entries by threat score.
Threat Weight	Displays the threat weight profile associated with the selected session.

Column name	Description
Timestamp	Displays the selected session's PHP timestamp.
User **User Name**	Displays the user name associated with the selected administrator.
Videos Played	Displays the number of videos played via cloud applications. **Note:** This column is only available in the **Cloud Applications** console.
VPN	Displays the Virtual Private Networks (VPNs) connected to the FortiGate, by name. **Note:** This column is only available in the **All Sessions** console.
VPN Type	Displays the type of VPN protocol (eg. PPTP, L2TP) in use by the associated connection.

Risk level indicators

There are currently two consoles within FortiView that display the Risk associated with the console: Applications and Cloud Applications. Each application pose different levels of risk to the network, represented by a colour code.

The following table identifies each risk level, from least to most severe:

Indicator	Risk	Description
	**Green:** *Risk Level 1*	These applications have little to no risk level, with no assigned risk definition. Application file-sharing may result in data leakage, which would be a typical example of a low level risk. An example application would be the Google toolbar, or Dropbox.
	**Blue:** *Risk Level 2*	These applications have an elevated risk level and typically use excessive bandwidth. High bandwidth consumption can lead to increased operational costs. An example application would be Bittorrent.

Indicator	Risk	Description
	**Yellow:** *Risk Level 3*	These applications have a low risk level and are typically evasive. Evasive applications can lead to compliance risks, and could include applications such as JustinTV and GlypeProxy.
	**Orange:** *Risk Level 4*	These applications have a high risk level, and are defined as using both excessive and evasive bandwidth. Example applications would be AutoHideIP and PandoraTV.
	**Red:** *Risk Level 5*	Applications that have a high risk level are prone to malware or vulnerabilities that can introduce business continuity risks.

Troubleshooting FortiView

FortiView does not display all consoles listed in this document

Some consoles require disk logging to be enabled before they will appear in FortiView. These include:

- Admin Logins
- Cloud Applications
- FortiSandbox
- Sources
- System Events
- Threats
- VPN
- Web Sites

Only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 7 for more information.

No logging data is displayed

In order for information to appear in the FortiView consoles, disk logging must be selected for the FortiGate unit. To select disk logging, go to **Log & Report > Log Config > Log Settings**.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

```
config log disk setting
   set status enable
end
```

Only certain FortiGate models support Disk Logging — refer to the FortiView Feature Support - Platform Matrix on page 7 for more information.

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.